DEPENDENCY-CHECK

How to read the report | **Suppressing false positives** | **Getting Help: google group** | **github issues**

Project: OWASP Threat Dragon

Scan Information (show all):

- *dependency-check version*: 2.1.1
- *Report Generated On*: Oct 2, 2017 at 14:03:21 +07:00
- *Dependencies Scanned*: 67 (1 unique)
- *Vulnerable Dependencies*: 1
- *Vulnerabilities Found*: 5
- *Vulnerabilities Suppressed*: 0
- ...

Display: Showing Vulnerable Dependencies (click to show all)

Dependency	CPE	GAV	Highest Severity	CVE Count	CPE Confidence	Evidence Count
owasp-threat-dragon/package.json			High	5		7

Dependencies

owasp-threat-dragon/package.json

License:

```
Apache-2.0
```

File Path: /Users/sprasanphani/git/owasp-threat-dragon/package.json
MD5: 8a2f99bc17f36cfc62689343d1996f0f
SHA1: bd7e9d4e35359081b89d51c5a514f14a3dfbb249

Evidence

Related Dependencies

Identifiers

- **None**

Published Vulnerabilities

NSP-535

Severity: High
CVSS Score: 7.5

The mime module is vulnerable to regular expression denial of service when a mime lookup is performed on untrusted user input.

- NSP - Advisory 535: Regular Expression Denial of Service

Vulnerable Software & Versions:

- mime:< 1.4.1 || > 2.0.0 < 2.0.3

NSP-534

Severity: Low
CVSS Score: 3.7

The debug module is vulnerable to regular expression denial of service when untrusted user input is passed into the `o` formatter. It takes around 50k characters to block for 2 seconds making this a low severity issue.

- NSP - Advisory 534: Regular Expression Denial of Service

Vulnerable Software & Versions:

- debug:<= 2.6.8 || >= 3.0.0 <= 3.0.1

NSP-526

Severity: High
CVSS Score: 7.5

Fresh is a module used by the Express.js framework for 'HTTP response freshness testing'. It is vulnerable to a regular expression denial of service when it is passed specially crafted input to parse. This causes the event loop to be blocked causing a denial of service condition.

- NSP - Advisory 526: Regular Expression Denial of Service

Vulnerable Software & Versions:

- fresh:< 0.5.2

NSP-48

Severity: Medium
CVSS Score: 5.3

uglify-js is vulnerable to regular expression denial of service (ReDoS) when certain types of input is passed into .parse(). "The Regular expression Denial of Service (ReDoS) is a Denial of Service attack, that exploits the fact that most Regular Expression implementations may reach extreme situations that cause them to work very slowly (exponentially related to input size). An attacker can then cause a program using a Regular Expression to enter these extreme situations and then hang for a very long time." [1] ### Proof of Concept ``` var u = require('uglify-js'); var genstr = function (len, chr) { var result = ""; for (i=0; i<=len; i++) { result = result + chr; } return result; } u.parse("var a = " + genstr(process.argv[2], "1") + ".1ee7;"); ``` ### Results ``` $ time node test.js 10000 real 0m1.091s user 0m1.047s sys 0m0.039s $ time node test.js 80000 real 0m6.486s user 0m6.229s sys 0m0.094s ```

- NSP - Advisory 48: Regular Expression Denial of Service

Vulnerable Software & Versions:

- uglify-js:<2.6.0

NSP-328

Severity: High
CVSS Score: 7.2

Jquery is a javascript library for DOM traversal and manipulation, event handling, animation, and Ajax. When text/javascript responses are received from cross-origin ajax requests not containing the option `dataType`, the result is executed in `jQuery.globalEval` potentially allowing an attacker to execute arbitrary code on the origin.

- NSP - Advisory 328: Cross-Site Scripting (XSS)

Vulnerable Software & Versions:

- jquery:>=1.4.0 <=1.11.3 || >=1.12.4 <=2.2.4

This report contains data retrieved from the National Vulnerability Database.
This report may contain data retrieved from the Node Security Platform.